UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/666,207	09/18/2003	Laurent Eschenauer	MR2833-34	8288

4586 7590 03/28/2008

ROSENBERG, KLEIN & LEE
3458 ELLICOTT CENTER DRIVE-SUITE 101
ELLICOTT CITY, MD 21043

EXAMINER	
PATEL, NIRAV B	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
03/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/666,207	ESCHENAUER ET AL.	
	Examiner	Art Unit	
	NIRAV PATEL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2007 (RCE)*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17 and 19-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,13,15,16 and 22* is/are rejected.

7)☐ Claim(s) *2-12, 14, 17, 19-21* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's submission for RCE filed on Dec. 21, 2007 has been entered. Claims 1-17, 19-22 are pending. Claims 1-5, 8, 9, 13, 16, 17 and 19 are amended and claim 18 are cancelled by the applicant.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech et al (US Patent No. 6,650,753) and in view of Rolf Blom ("An optimal class of symmetric key generation system" 1998).

As per claim 1, Lotspiech teaches:

prior to deployment of a plurality of sensor nodes of the Distributed Sensor Network, storing, a respective key ring including a plurality of individually selectable private keys in each sensor node of the Distributed Sensor Network, said private keys being randomly chosen from a common pool [Fig. 4, 3, 5, col. 20-28, 32-67, col. 6 lines 1-15, col. 6 lines 42-50]; deploying said plurality of the sensor nodes of the Distributed Sensor Network; actuating upon deployment of said plurality of the sensor nodes of the Distributed Sensor Network, at least one sensor node to discover at least another sensor node sharing said at least one private key to establish a secure communication link between said one sensor node and another of said sensor nodes; and using said at least one shared private key for subsequent secure communication between said at least one sensor node and said other sensor node [Fig. 4, col. 5 lines 66-67, col. 6 lines 1-16, 39-50].

Rolf Blom teaches: said key rings of at least a pair of said sensor nodes having a pre-defined probability of having at least one common private key in common [page 336, Introduction].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Rolf Blom with Lotspiech, since one would have been motivated to resolve the uncertainty of unknown keys [Rolf Blom, page 335 abstract lines 12-13].

3. Claims 13 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech et al (US Patent No. 6,650,753) in view of Rolf Blom ("An optimal class of symmetric key generation system" 1998) and in view of Huitema et al (US Patent No. 7,068789).

As per claim 13, the rejection of claim 1 is incorporated and Huitema teaches:

upon expiration of at least one key shared by said at least one and other sensor node, removal of said expired at least one key from said key rings of said at least one and other sensor nodes, and searching for other key common for said at least one and other sensor nodes to establish a new communication link therebetween [Fig. 4-6, col. 10 lines 16-45, col. 12 lines 1-67, col. 15 lines 21-60].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Huitema with Lotspiech and Rolf Blom, since one would have been motivated to provide security framework that address the threats at a group level that can adversely affect the peer-to-peer group [Huitema, col. 2 lines 51-54].

As per claim 16, Lotspiech teaches:

at least two sensor nodes, each said sensor node being pre-loaded prior to deployment thereof with a respective key ring including a plurality of individually selectable private keys randomly chosen from a common pool, each of said private keys of said key ring having an associated key identifier stored in a corresponding sensor node [Fig. 4, 3, 5, col. 20-28, 32-67, col. 6 lines 1-15, col. 6 lines 42-50].

Rolf Blom teaches:

the key rings of at least a pair of said sensor nodes having a pre-defined probability of having at least one common private key in common[page 336, Introduction].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Rolf Blom with Lotspiech, since one would have been motivated to resolve the uncertainty of unknown keys [Rolf Blom, page 335 abstract lines 12-13].

Huitema teaches:

each of said sensor nodes having means for searching for another sensor node where a plurality of said key identifiers are broadcast to search for other sensor nodes with a matching of at least one of the key identifiers, said matching key identifier indicating the other sensor node has a private key in common key therewith to establish a secure communication link therebetween [Fig. 4-6, col. 12 lines 46-67, col. 13 lines 40-67, col. 14 lines 1-43].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Huitema with Lotspiech and Rolf Blom, since one would have been motivated to provide security framework that address the threats at a group level that can adversely affect the peer-to-peer group [Huitema, col. 2 lines 51-54].

4. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech et al (US Patent No. 6,650,753) in view of Rolf Blom ("An optimal class of symmetric key generation system" 1998) and in view of Kasahara et al. (U. S. Patent No. 6,788,788).

As per claim 15, the rejection of claim 1 is incorporated and Kasahara teaches:

assigning a path-key to a selected pair of sensor nodes connected by at least two communication links [Fig. 1, col. 4 lines 1-60, col. 8 lines 45-50].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kasahara with Lotspiech and Rolf Blom, since one would have been motivated to provide high degree of security [col. 3 line 38].

5. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech et al (US Patent No. 6,650,753) in view of Rolf Blom ("An optimal class of symmetric key generation system" 1998) in view of Huitema et al (US Patent No. 7,068789) and in view of Kasahara et al. (U. S. Patent No. 6,788,788).

As per claim 22, the rejection of claim 16 is incorporated and Kasahara teaches:

assigning a path-key to a selected pair of sensor nodes connected by at least two communication links [Fig. 1, col. 4 lines 1-60, col. 8 lines 45-50].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kasahara with Lotspiech, Rolf Blom and Huitema, since one would have been motivated to provide high degree of security [col. 3 line 38].

Allowable Subject Matter

6. Claims 2-12, 14, 17, 19-21 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Amendment

7. This written action is responding to the Request for Continued Examination (RCE) dated Dec. 21, 2007. Applicant has amended claims 1 and 16, which necessitated new ground of rejection. See new ground of rejection above. Therefore, the applicant's arguments, filed on Dec. 21, 2007, are moot in view of the new ground(s) of rejection

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Grumiaux (US 2003/0133576) – Generation of a common encryption key

Baugher et al (US 7234063) – Method and Apparatus for generating pairwise cryptographic transforms based on group keys

Au et al (US 7120696) – Cryptographic communications using pseudo-randomly generated cryptography keys

Boneh et al (US 2003/0081785) -- Systems and methods for identity-based encryption and related cryptographic techniques

Hengeveld et al (US 2004/0054891) – Secure encryption key distribution

Arakawa et al (US 2003/0021418) – Cryptogram communication system

Any inquiry concerning this communication or earlier communications from the examiner should be directed to NIRAV PATEL whose telephone number is (571)272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NP
3/24/08
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135